US006084965A

United States Patent [19]

Ahn et al.

[11] Patent Number: 6,084,965

[45] Date of Patent: Jul. 4, 2000

[54] **IDENTIFICATION SCHEME, DIGITAL SIGNATURE SCHEME GIVING MESSAGE RECOVERY AND DIGITAL SIGNATURE SCHEME WITH APPENDIX**

[75] Inventors: **Keum Hyug Ahn**; **Yun Ho Lee**; **Ill Hwan Park**; **Chung Ryong Jang**, all of Seoul, Rep. of Korea

[73] Assignee: **Korea Telecommunication Authority**, Seoul, Rep. of Korea

[21] Appl. No.: **08/649,457**

[22] Filed: **May 17, 1996**

[30] **Foreign Application Priority Data**

May 17, 1995 [KR] Rep. of Korea 95-12289

[51] **Int. Cl.**[7] **H04K 1/00**; H04L 9/00

[52] **U.S. Cl.** **380/28**; 380/25

[58] **Field of Search** 380/4, 21, 28, 380/29, 30, 25

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,625,076	11/1986	Okamoto et al.	178/22.11
4,969,189	11/1990	Ohta et al.	380/25
5,140,634	8/1992	Guillou et al.	380/23
5,396,558	3/1995	Ishiguro et al.	380/25
5,442,707	8/1995	Miyaji et al.	380/30
5,446,796	8/1995	Ishiguro et al.	380/24
5,483,597	1/1996	Stern	380/30

Primary Examiner—Max Noori

Attorney, Agent, or Firm—Merchant & Gould P.C.

[57] **ABSTRACT**

An identification scheme, a digital signature scheme giving message recovery, and a digital signature scheme with appendix are disclosed. In processing and transmitting information, a transmitting counterpart of a transmission message is confirmed. The unauthorized modification of the message is confirmed and transmitting behavior is detected, thereby providing the reliable information service.

12 Claims, 3 Drawing Sheets

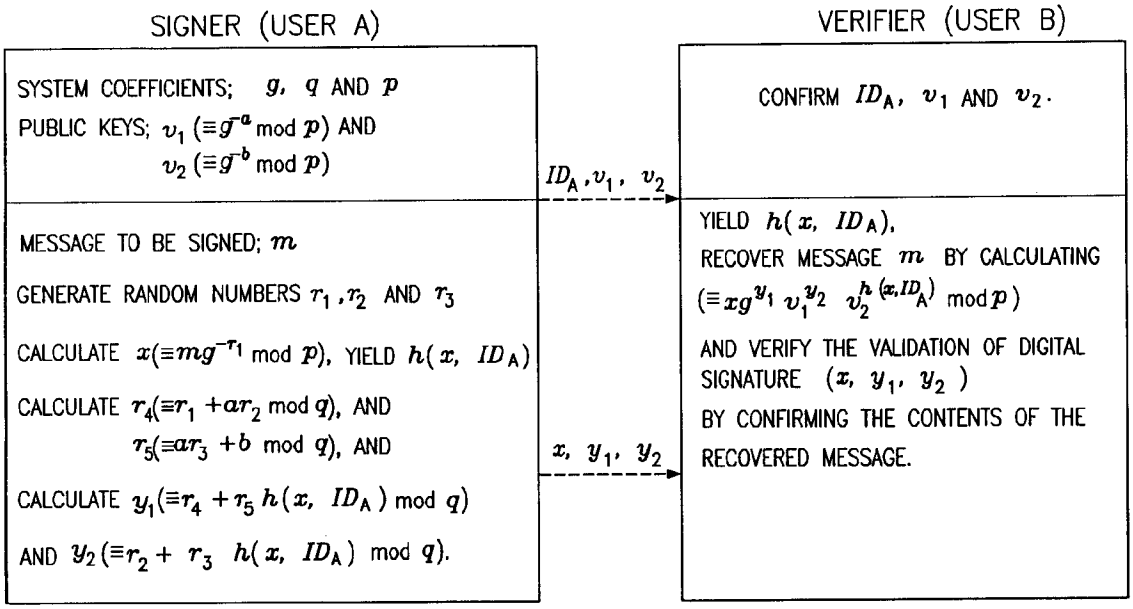


FIG. 1

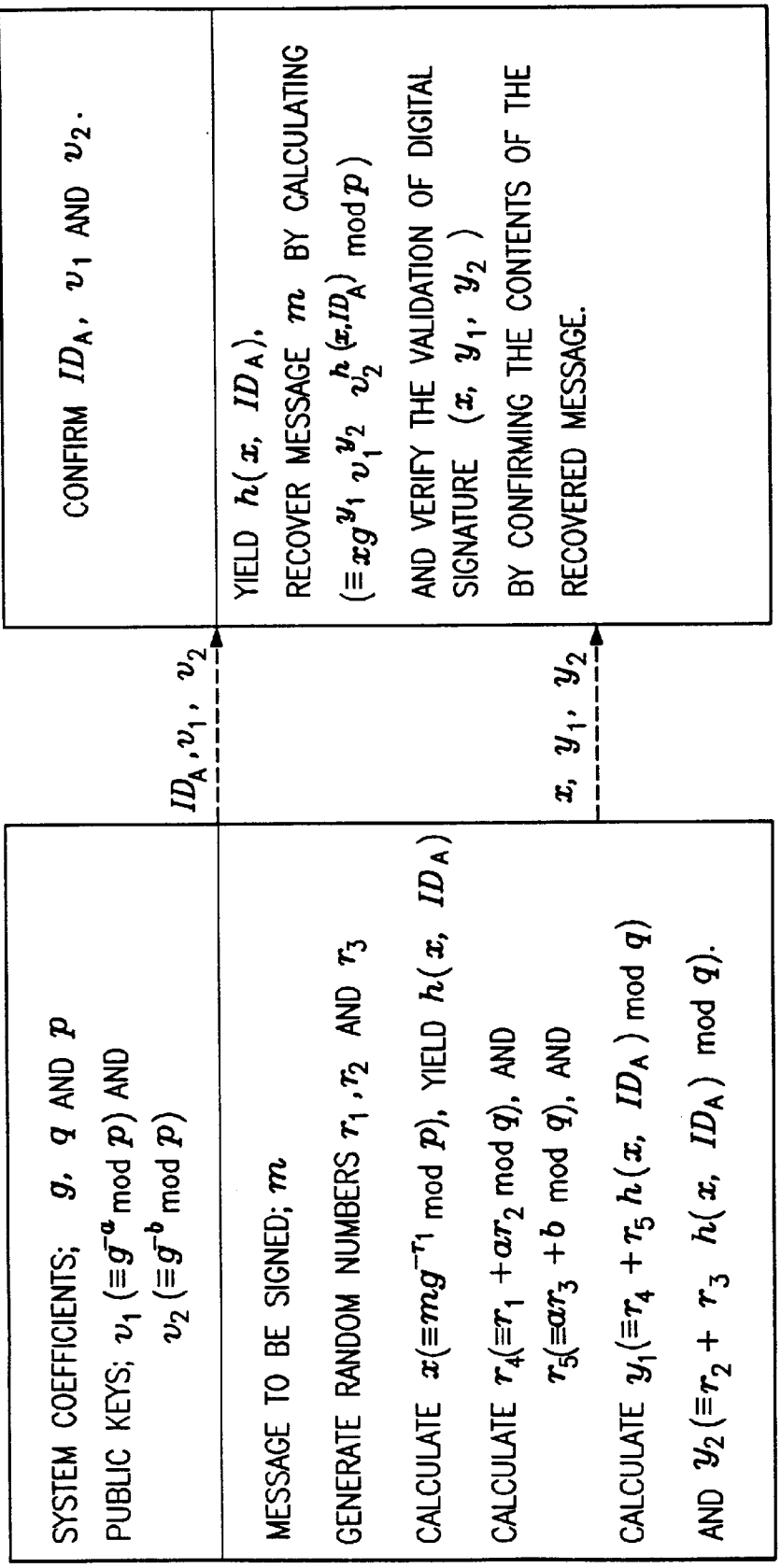

SIGNER (USER A)
SYSTEM COEFFICIENTS; g, q AND p
PUBLIC KEYS; v1 (≡g^-a mod p) AND
v2 (≡g^-b mod p)
MESSAGE TO BE SIGNED; m
GENERATE RANDOM NUMBERS r1, r2 AND r3
CALCULATE x(≡mg^-r1 mod p), YIELD h(x, IDA)
CALCULATE r4(≡r1 +ar2 mod q), AND
r5(≡ar3 +b mod q), AND
CALCULATE y1(≡r4 + r5 h(x, IDA) mod q)
AND y2 (≡r2 + r3 h(x, IDA) mod q).
IDA, v1, v2
x, y1, y2
VERIFIER (USER B)
CONFIRM IDA, v1 AND v2.
YIELD h(x, IDA),
RECOVER MESSAGE m BY CALCULATING
(≡xg^y1 v1^y2 v2^h(x,IDA) mod p)
AND VERIFY THE VALIDATION OF DIGITAL
SIGNATURE (x, y1, y2)
BY CONFIRMING THE CONTENTS OF THE
RECOVERED MESSAGE.

FIG. 2

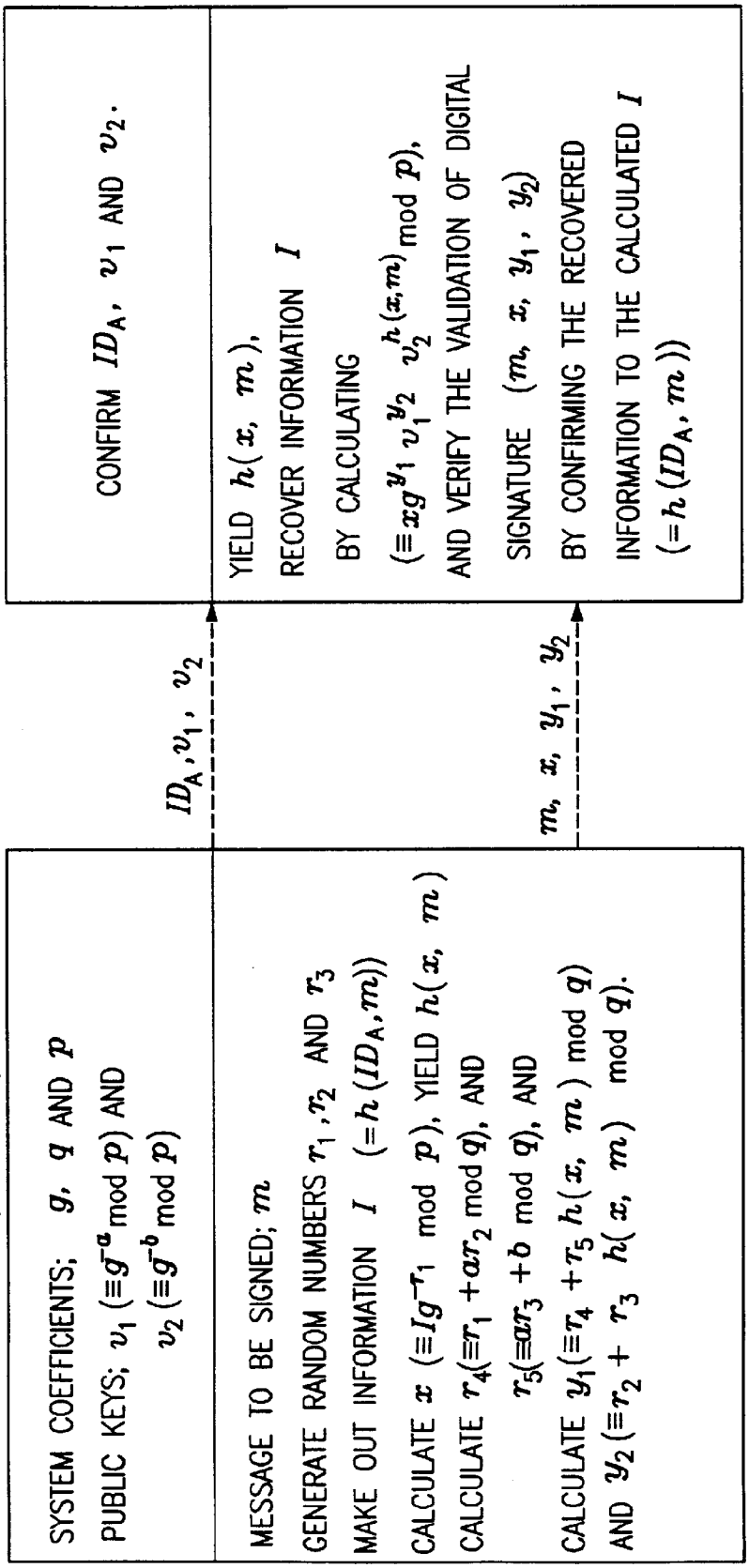
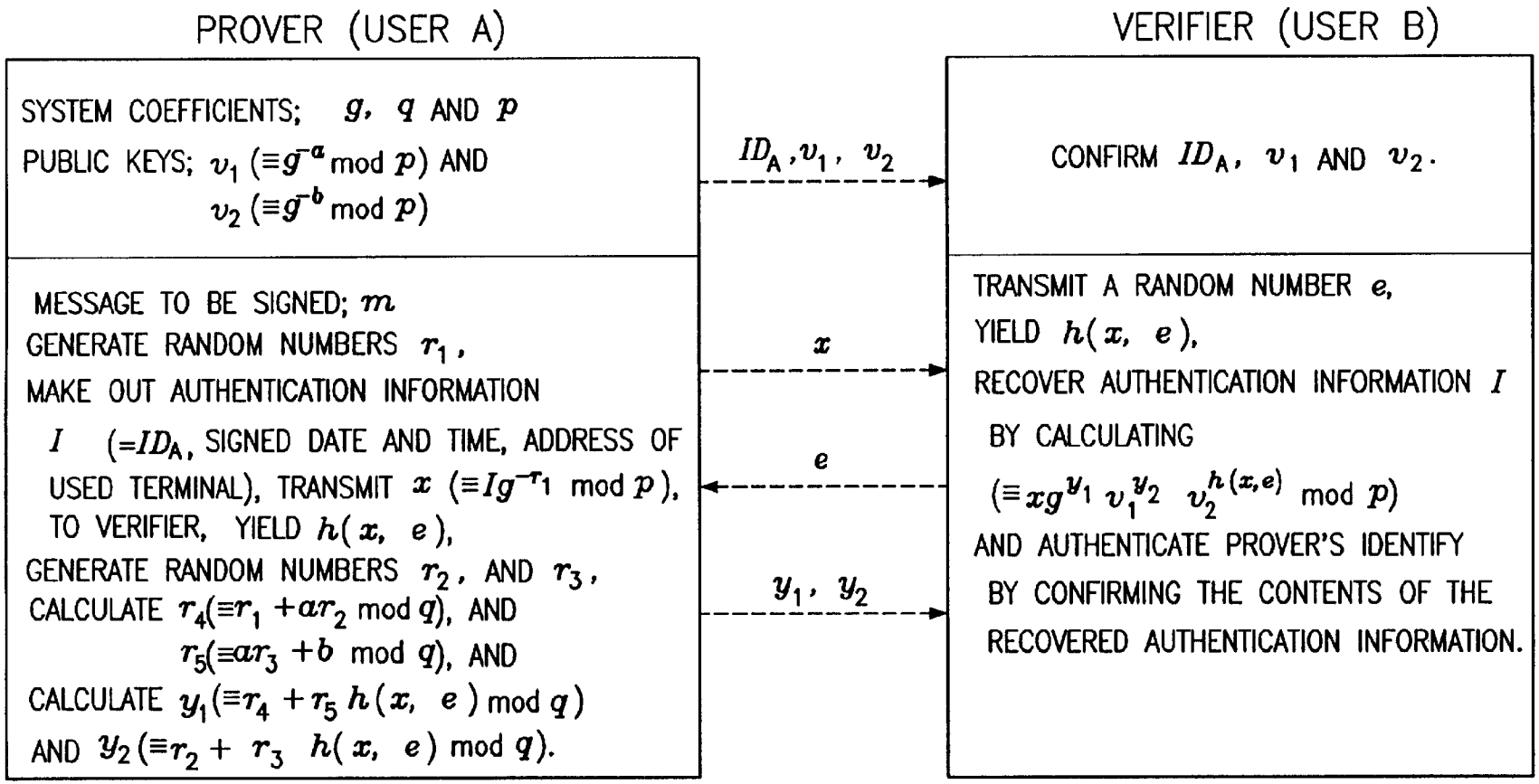

SIGNER (USER A)
SYSTEM COEFFICIENTS; g, q AND p
PUBLIC KEYS; v_1 ($\equiv g^{-a} \bmod p$) AND
v_2 ($\equiv g^{-b} \bmod p$)
MESSAGE TO BE SIGNED; m
GENERATE RANDOM NUMBERS r_1, r_2 AND r_3
MAKE OUT INFORMATION I ($=h(ID_A, m)$)
CALCULATE x ($\equiv Ig^{r_1} \bmod p$), YIELD $h(x, m)$
CALCULATE r_4($\equiv r_1 + ar_2 \bmod q$), AND
r_5($\equiv ar_3 + b \bmod q$), AND
CALCULATE y_1($\equiv r_4 + r_5 h(x, m) \bmod q$)
AND y_2 ($\equiv r_2 + r_3 h(x, m) \bmod q$).
ID_A, v_1, v_2
m, x, y_1, y_2
VERIFIER (USER B)
CONFIRM ID_A, v_1 AND v_2.
YIELD $h(x, m)$,
RECOVER INFORMATION I
BY CALCULATING
($\equiv xg^{y_1} v_1^{y_2} v_2^{h(x,m)} \bmod p$),
AND VERIFY THE VALIDATION OF DIGITAL
SIGNATURE (m, x, y_1, y_2)
BY CONFIRMING THE RECOVERED
INFORMATION TO THE CALCULATED I
($=h(ID_A, m)$)

FIG. 3


PROVER (USER A)
VERIFIER (USER B)
SYSTEM COEFFICIENTS; g, q AND p
PUBLIC KEYS; v1 (≡g^-a mod p) AND
v2 (≡g^-b mod p)
ID_A, v1, v2
CONFIRM ID_A, v1 AND v2.
MESSAGE TO BE SIGNED; m
GENERATE RANDOM NUMBERS r1,
MAKE OUT AUTHENTICATION INFORMATION
I (=ID_A, SIGNED DATE AND TIME, ADDRESS OF USED TERMINAL), TRANSMIT x (≡Ig^-r1 mod p), TO VERIFIER, YIELD h(x, e),
GENERATE RANDOM NUMBERS r2, AND r3,
CALCULATE r4(≡r1 + ar2 mod q), AND
r5(≡ar3 + b mod q), AND
CALCULATE y1(≡r4 + r5 h(x, e) mod q)
AND y2(≡r2 + r3 h(x, e) mod q).
x
e
y1, y2
TRANSMIT A RANDOM NUMBER e,
YIELD h(x, e),
RECOVER AUTHENTICATION INFORMATION I
BY CALCULATING
(≡xg^y1 v1^y2 v2^h(x,e) mod p)
AND AUTHENTICATE PROVER'S IDENTIFY
BY CONFIRMING THE CONTENTS OF THE
RECOVERED AUTHENTICATION INFORMATION.

IDENTIFICATION SCHEME, DIGITAL SIGNATURE SCHEME GIVING MESSAGE RECOVERY AND DIGITAL SIGNATURE SCHEME WITH APPENDIX

BACKGROUND OF THE INVENTION

The present invention relates to an identification scheme based on security according to difficulty in calculating discrete logarithms, and a digital signature scheme giving message recovery and a digital signature scheme with appendix for authenticating each identity processing information, protecting the integrity of transferred information and preventing fraudulent information processing behavior.

A digital signature corresponding to a conventional manual signature is used to confirm a communicating counterpart, to prevent the unauthorized modification of the communication contents and to solve a dispute about communication behavior. A method for generating the digital signature can be classified into a digital signature scheme with appendix and a digital signature scheme giving message recovery, according to forms and functions of the generated digital signature.

Assuming that p is a large prime number, q is another prime number for dividing p−1, g is a natural number having a remainder 1 obtained by dividing its q^{th} power by p, g being between 1 and p, then g, q and p are system coefficients commonly utilized by users. If each user randomly selects a natural number s between 1 and q as a secret key and uses, as a public key, a remainder v ($\equiv g^{-s} \bmod p$) obtained by dividing the $-s^{th}$ power of g by p, public coefficients used by each user are v, g, q and p.

It is hard to find out the secret key s from these public coefficients and therefore it is equivalent that a problem of discrete logarithms is difficult to calculate. Numerous public key identification schemes and digital signature schemes are based on security strength from the fact that the problem of the discrete logarithms is difficult to calculate.

Schnorr published the identification scheme and the digital signature scheme based on the security of the discrete logarithms in 1989. The digital signature scheme published by Schnorr, which is the digital signature scheme with appendix, introduces a hash compression function to the digital signature scheme published by Elgamal in 1985, and simplifies the procedure for generating and verifying the digital signature. Moreover, the generated digital signature is small in size.

The identification scheme proposed by Schnorr uses the same logarithm structure as the digital signature scheme, and authenticates one's own identity to a communicating counterpart.

The identification scheme proposed by Schnorr in which a prover A authenticates his identity to a verifier B will now be described.

If the prover's system coefficients are g, q and p, the secret key is s (1<s<q), and the public key is v ($\equiv g^{-s} \bmod p$), the prover A selects a random number r between 1 and g and transmits a remainder x ($\equiv g^{r} \bmod p$) obtained by dividing the r^{th} power of g by p to the verifier B. If x is received from the prover A, the verifier B selects a random number e between 1 and q and transmits the number e to the prover A. The prover A multiplies the random number e received from the verifier B by the secret key s and adds the random number r, to yield r+se. The prover A transmits a remainder y ($\equiv$r+se mod q) obtained by dividing r+se by q to the verifier B. If y is received from the prover A, the verifier B calculates a remainder x' ($\equiv g^{y} v^{e} \bmod p$) obtained by dividing the product of the y^{th} power of g and the e^{th} power of v by p. The verifier B authenticates the validation of prover's identity by confirming whether x' and x are identical to each other.

In the digital signature scheme with appendix proposed by Schnorr, if a message to be signed is m, a signer A selects a random number r between 1 and q and calculates a remainder x ($\equiv g^{r} \bmod p$) obtained by dividing the r^{th} power of g by p. The message m and the calculated x are applied to the hash function to yield e (=h(x, m)). The signer A calculates a remainder y ($\equiv$r+se mod q) obtained by dividing r added to the product of s and e by q. Then (e, y) is the digital signature with appendix for the message m. The validation of the digital signature (e, y) with appendix for the message m is easily verified since a singer's public key is known.

That is, if the digital signature with appendix of the signer A for the message m is (e, y), the verifier B calculates a remainder x' ($\equiv g^{y} v^{e} \bmod p$) obtained by dividing the product of the y^{th} power of g and the e^{th} power of v by p. The remainder x' and the message m are applied to the hash function to yield e' (=h(x', m). The validation of the digital signature (e, y) with appendix of the signer A is verified by confirming whether e' and e are the same.

Meanwhile, Nyberg and Rueppel published the digital signature scheme giving message recovery based on security of the discrete logarithms in 1993. The digital signature scheme giving message recovery of N-R (Nyberg-Rueppel) will now be described.

It is assumed that the signer's system coefficients are g, q and p, the secret key is s (1<s<q), the public key is v ($\equiv g^{-s} \bmod p$), and the message to be signed is m, m being a natural number which is greater than or equal to 1, and less than or equal to the prime number p. The signer selects a random number r between 1 and q, and calculates a remainder x ($\equiv mg^{-r} \bmod p$) obtained by dividing the product of the message m and the $-r^{th}$ power of g by p. The singer adds r to the secret key s multiplied by x to yield r+sx and calculates a remainder y ($\equiv$r+sx mod q) obtained by dividing r+sx by q. Then (x, y) is the digital signature giving message recovery for the message m.

To verify the digital signature (x, y), the verifier calculates a remainder($\equiv xg^{y} v^{x} \bmod p$) obtained by dividing the product of x and the y^{th} power of g and the x^{th} power of v by p, to recover the message m. The verifier verifies the validation of the digital signature (x, y) by confirming the contents of the recovered message m.

However, the digital signature with appendix generates only the digital signature for the message. In the digital signature giving message recovery, if the message to be signed is larger in size than p, the message m should be divided into various messages smaller than p. Since the digital signature is generated for the divided messages, the size of the generated digital signature is increased.

SUMMARY OF THE INVENTION

It is therefore an object of the invention to provide an identification scheme for confirming a communicating counterpart of a transmission message in processing and transmitting information.

It is another object of the invention to provide a digital signature scheme giving message recovery for confirming the unauthorized modification of a message and detecting transmitting behavior.

It is still another object of the invention to provide a digital signature scheme with appendix for confirming the

unauthorized modification of a message and detecting transmitting behavior.

In accordance with one aspect of the invention, a method for generating a digital signature giving message recovery and verifying the generated digital signature when system coefficients are g, q and p, comprising the steps of:

(for a signer) selecting a first random number r1, calculating a first remainder x ($\equiv mg^{-r1} \bmod p$) obtained by dividing the product of a message m and the $-r1^{th}$ power of g by p, and applying said first remainder x and a singer's identification ID to a hash function to yield h(x, ID);

(for said signer) selecting second and third random numbers r2 and r3, calculating a second remainder r4 ($\equiv r1+ar2 \bmod q$) obtained by dividing, by q, said first random number r1 added to the product of a first secret key a and said second random number r2, and calculating a third remainder r5 ($\equiv ar3+b \bmod q$) obtained by dividing, by q, a second secret key b added to the product of said first secret key a and said third random number r3;

calculating a fourth remainder y1 ($\equiv r4+r5\ h(x, ID) \bmod q$) obtained by dividing, by q, said second remainder r4 added to the product of said third remainder r5 and h(x, ID), and calculating a fifth remainder y2 ($\equiv r2+r3\ h(x, ID) \bmod q$) obtained by dividing, by q, said second random number r2 added to the product of said third random number r3 and h(x, ID), thus to generate a digital signature (x, y1, y2) for said message m;

(for a verifier) applying said first remainder x and said signer's identification ID to said hash function to yield h(x, ID); and

recovering said message m contained in said first remainder x by calculating a remainder ($\equiv xg^{y1}v1^{y2}v2^{h(x,\ ID)} \bmod p$) obtained by dividing, by p, the product of said first remainder x and the $y1^{th}$ power of g and the $y2^{th}$ power of a first public key v1 ($\equiv g^{-a} \bmod p$) and the $\{h(x, ID)\}^{th}$ power of a second public key v2 ($\equiv g^{-b} \bmod p$), and verifying the validation of said digital signature (x, y1, y2) by confirming the contents of the recovered message.

In accordance with another aspect of the invention, a method for generating a digital signature with appendix and verifying the generated digital signature when system coefficients are g, q and p, comprising the steps of:

(for a signer) selecting a first random number r1, applying a message m and a signer's identification ID to a hash function to yield h(ID, m), calculating a first remainder x ($\equiv h(ID, m)g^{-r1} \bmod p$) obtained by dividing, by p, the product of h(ID, m) and the $-r1^{th}$ power of g, and applying said first remainder x and said message m to said hash function to yield h(x, m);

selecting second and third random numbers r2 and r3, calculating a second remainder r4 ($\equiv r1+ar2 \bmod q$) obtained by dividing, by q, said first random number r1 added to the product of a first secret key a and said second random number r2, and calculating a third remainder r5 ($\equiv ar3+b \bmod q$) obtained by dividing, by q, a second secret key b added to the product of said first secret key a and said third random number r3;

calculating a fourth remainder y1 ($\equiv r4+r5\ h(x, m) \bmod q$) obtained by dividing, by q, said second remainder r4 added to the product of said third remainder r5 and h(x, m), and calculating a fifth remainder y2 ($\equiv r2+r3\ h(x, m) \bmod q$) obtained by dividing, by q, said second random number r2 added to the product of said third random number r3 and h(x, m), thus to generate a digital signature (x, y1, y2) for said message m;

(for a verifier) applying said first remainder x and said message m to said hash function to yield h(x, m), and recovering h(ID, m) by calculating a sixth remainder ($\equiv xg^{y1}v1^{y2}v2^{h(x,\ m)} \bmod p$) obtained by dividing, by p, the product of said first remainder x and the $y1^{th}$ power of g and the $y2^{th}$ power of a first public key v1 ($\equiv g^{-a} \bmod p$) and the $\{h(x, m)\}^{th}$ power of a second public key v2 ($\equiv g^{-b} \bmod p$); and

verifying the validation of said digital signature (x, y1, y2) by confirming whether the recovered h(ID, m) is equal to h(x, ID) obtained by applying said signer's identification ID and said message m to said hash function.

In accordance with still another aspect of the invention, a method for authenticating user's identity when system coefficients are g, q and p, comprising the steps of:

(for a prover) selecting a first random number r1, making out authentication information I including a prover's identification and a current time, transmitting a first remainder x ($\equiv Ig^{-r1} \bmod p$) obtained by dividing the product of said authentication information I the $-r1^{th}$ power of g by p to a verifier, and (for said verifier) transmitting a second random number e to said prover;

(for said prover) applying said first remainder x and said second random number e to said hash function to yield h(x, e), selecting second and third random numbers r2 and r3, calculating a second remainder r4 ($\equiv r1+ar2 \bmod q$) obtained by dividing, by g, said first random number r1 added to the product of a first secret key a and said second random number r2, and calculating a third remainder r5 ($\equiv ar3+b \bmod q$) obtained by dividing, by q, a second secret key b added to the product of said first secret key a and said third random number r3; and

calculating a fourth remainder y1 ($\equiv r4+r5\ h(x, e) \bmod q$) obtained by dividing, by q, said second remainder r4 added to the product of said third remainder r5 and h(x, e), and calculating a fifth remainder y2 ($\equiv r2+r3\ h(x, e) \bmod q$) obtained by dividing, by q, said second random number r2 added to the product of said third random number r3 and h(x, e), thus to generate a digital signature (x, y1, y2) for said message m;

(for said verifier) recovering said authentication information I contained in said first remainder x by calculating a remainder ($\equiv xg^{y1}v1^{y2}v2^{h(x,\ e)} \bmod p$) obtained by dividing, by p, the product of said first remainder x and the $y1^{th}$ power of g and the $y2^{th}$ power of a first public key v1 ($\equiv g^{-a} \bmod p$) and the $\{h(x, e)\}^{th}$ power of a second public key v2 ($\equiv g^{-b} \bmod p$), and authenticating prover's identity by confirming the contents of the recovered authentication information.

The present invention is more specifically described with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE ATTACHED DRAWINGS

FIG. **1** shows a process for a digital signature scheme giving message recovery according to the present invention;

FIG. **2** shows a process for a digital signature scheme with appendix according to the present invention; and

FIG. **3** shows a process for an identification scheme according to the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENT

Referring to FIG. **1**, each user has two secret keys and two public keys corresponding thereto, and can generate a digital

signature for a message to be signed. If the message to be signed is m, the signer's secret keys are a and b, and the public keys are v1 ($\equiv g^{-a} \bmod p$) and v2 ($\equiv g^{-b} \bmod p$), each user commonly uses a hash function h and system coefficients g, q and p. When using a digital signature scheme, a unique identification (ID) is assigned to each user from a key authentication center.

A signer A selects a random number r1 between 1 and q and calculates a remainder x ($\equiv mg^{-r1} \bmod p$) obtained by dividing the product of the message m and the $-r_1{}^{th}$ power of g by p. The signers A applies the remainder x and his identification ID_A to the hash function to yield $h(x, ID_A)$. The signer A selects random numbers r2 and r3 between 1 and q, and calculates r4 ($\equiv r1+ar2 \bmod q$), r5 ($\equiv ar3+b \bmod q$), y1 ($\equiv r4+h(x, ID_A)r5 \bmod q$), and y2 ($\equiv r2+h(x, ID_A)r3 \bmod q$).

Instead of calculating y1 and y2 using $h(x, ID_A)$ after the random numbers r2 and r3 are selected, and r4 and r5 are calculated using the secret keys a and b, one random number r2 may be selected as y2, and y1 may be calculated using the secret keys a and b and the calculated $h(x, ID_A)$. That is, the signer A selects the random number r2 between 1 and q as y2. Then y1 is calculated by the following expression $y1 \equiv r1+h(x, ID_A)b+ay2 \bmod q$. Thus, the obtained value (x, y1, y2) is the digital signature giving message recovery for the message m.

To verify the digital signature (x, y1, y2), a verifier B applies x and the signer's identification ID_A to the hash function to yield $h(x, ID_A)$. The message m is recovered by calculating a remainder ($\equiv xg^{y1}v1^{y2}v2^{h(x,IDA)} \bmod p$) obtained by dividing, by p, the product of x and the $y1^{th}$ power of g and the $y2^{th}$ power of the public key v1 and the $\{h(x, ID_A)\}^{th}$ power of the public key v2. The verifier B verifies the validation of the signature for the message m by confirming the contents of the recovered message m.

FIG. **2** shows a process for a digital signature scheme with appendix according to the present invention. The generated digital signature is added to the end of a signed message and is processed in pairs together with the signed message.

The signer A applies his identification ID_A and the message m to the hash function to yield I ($=h(ID_A, m)$). The signer also makes out I by appending the security related data, e.g. the description for the corresponding message and the time when the digital signature is generated through a computer terminal. The signer A selects a random number r1 between 1 and q, and calculates a remainder x ($\equiv Ig^{-r1} \bmod p$) obtained by dividing the product of I and the $-r1^{th}$ power of g by p. The signer A applies x and the message m to the hash function to yield h(x, m). The signer A selects random numbers r2 and r3 between 1 and q and calculates r4 ($\equiv r1+ar2 \bmod q$), r5 ($\equiv ar3+b \bmod q$), y1 ($\equiv r4+h(x, m)r5 \bmod q$) and y2 ($\equiv r2+h(x, m)r3 \bmod q$).

Instead of calculating y1 and y2 using h(x, m) after the random numbers r2 and r3 are selected, and r4 and r5 are calculated using the secret keys a and b, one random number r2 may be selected as y2, and y1 may be calculated using the secret keys a and b, and h(x, m). In more detail, the signer A selects the random number r2 between 1 and q as y2. The remainder y1 is calculated by the following expression $y1 \equiv r1+h(x, m)b+ay2 \bmod q$. Thus (x, y1, y2) is the digital signature with appendix for the message m and is processed together with the message m as (m, x, y1, y2).

To verify the digital signature (m, x, y1, y2) with appendix, the verifier B calculates h(x, m) by applying x and the message m in the digital signature (m, x, y1, y2) to the hash function. I is recovered by calculating a remainder ($\equiv xg^{y1}v1^{y2}v2^{h(x, m)} \bmod p$) obtained by dividing, by p, the product of x and the $y1^{th}$ power of g and the $y2^{th}$ power of v1 and $\{h(x,m)\}^{th}$ power of v2. The verifier B applies the signer's identification ID_A and the message m to the hash function to obtain $h(ID_A, m)$. The validation of the digital signature with appendix for the message m is verified by confirming whether the obtained $h(ID_A, m)$ is equal to the recovered I.

Therefore, the digital signature giving message recovery and the digital signature with appendix are appropriately used according to the length of binary bit sequence of the message to be signed. If the size of the message is small, the signer uses the digital signature giving message recovery. Since the verifier can recover the signed message from the result of verifying the validation of the digital signature, the amount of communication between the signer and the verifier can be reduced. If the size of the message is large, the digital signature with appendix is used to generate the digital signature including information such as a description phrase of the signer, a signed time, etc.

That is, the signer applies his identification ID and the message m to the hash function to obtain h(ID, m). The signer appends the description phrase for the message m to h(ID, m). The signer makes out I ($=h(ID_A, Im)$, a description phrase, a signed time) by appending the description for the corresponding message and the time when the digital signature is generated through a computer terminal, and generates the digital signature with appendix.

FIG. **3** shows a process for an identification scheme according to the present invention. To enhance security, each user may use 2 secret keys, and 2 public keys corresponding thereto. Random numbers a and b between 1 and q are selected as the secret keys. The public keys are v1 ($\equiv g^{-a} \bmod p$) and v2 ($\equiv g^{-b} \bmod p$). To prove one's own identity to a verifier B, a prover A selects a random number r1 between 1 and q and calculates the $-r1^{th}$ power of g. The prover A makes out information I ($=ID_A$, signed date and time, address of used terminal, etc.) including his identification ID_A, the signed date and time, a host computer address or a node address indicating a position of a used terminal and the like, and transmits x ($\equiv Ig^{-r1} \bmod p$) to the verifier B. Authentification information I can be 1.

If x is received from the prover A, the verifier B selects a random number e between 1 and q and transmits the random number e to the prover A. The prover A applies e and x to the hash function to yield h(x, e). Numbers r2 and r3 between 1 and q are randomly selected by the prover A, and r4 ($\equiv r1+ar2 \bmod q$) and r5 ($\equiv ar3+b \bmod q$) are calculated. The prover A transmits y1 ($\equiv r4+h(x, e)r5 \bmod q$) and y2 ($\equiv r2+h(x, e)r3 \bmod q$) to the verifier B.

In the above description, y1 and y2 are calculated using h(x, e) after selecting the random numbers r2 and r3 and calculating r4 and r5 using the secret keys a and b. However, one random number r2 may be selected as y2, and y1 may be calculated using a and b, h(x, e). In more detail, the prover A selects the random number r2 between 1 and q as y2, and the remainder y1 is obtained by the following expression $y1 \equiv r1+h(x, e)b+ay2 \bmod q$. The prover A transmits y1 and y2 to the verifier B.

If y1 and y2 are received from the prover A, the verifier B recovers the authentication information I by calculating $xg^{y1}v1^{y2}v2^{h(x, e)} \bmod p$. The verifier B authenticates prover's identity by confirming the contents of the recovered authentication information I.

In the other hand, the random number $-r1$ can be used instead of the random number r1.

As described above, the reliable information service is possible and a communicating counterpart can be effectively authenticated.

What is claimed is:

1. A method for generating a digital signature giving message recovery and verifying the generated digital signature when system coefficients are g, q and p, wherein p and q are prime numbers different from each other, g is a natural number between 1 and p and a remainder obtained by dividing q^{th} power of g by p is 1, the method comprising the steps of:

for a signer, selecting a first random number r1, calculating a first remainder $x \equiv mg^{-r1} \bmod p$, wherein m is a message, and applying the first remainder x and a signer's identification ID to a hash function to generate h(x, ID);

for the signer, selecting second and third random numbers r2 and r3, calculating a second remainder $r4 \equiv r1+ar2 \bmod q$, wherein a is a first secret key, and calculating a third remainder $r5 \equiv ar3+b \bmod q$, wherein b is a second secret key;

calculating a fourth remainder $y1 \equiv r4+r5\ h(x, ID) \bmod q$ and calculating a fifth remainder $y2 \equiv r2+r3\ h(x, ID) \bmod q$, thus to generate a digital signature (x, y1, y2) for the message m;

for a verifier, applying the first remainder x and the signer's identification ID to the hash function to generate h(x, ID); and

recovering the message m contained in the first remainder x by calculating a remainder $\equiv xg^{y1}v1^{y2}v2^{h(x, ID)} \bmod p$, wherein y1 is a first public key, $v1 \equiv g^{-a} \bmod p$, v3 is a second public key and $v2 \equiv g^{-b} \bmod p$, and verifying the validation of the digital signature (x, y1, y2) by confirming the contents of the recovered message.

2. A method for generating a digital signature giving message recovery and verifying the generated digital signature when system coefficients are g, q and p, wherein p and q are prime numbers different from each other, g is a natural number between 1 and p and a remainder obtained by dividing g^{th} power by g by p is 1, the method comprising the steps of:

for a signer, selecting a first random number r1, calculating a first remainder $x \equiv mg^{-r1} \bmod p$, wherein m is a message, and applying the first remainder x and a signer's identification ID to a hash function to generate h(x, ID);

selecting a random number r2 between 1 and q to be used as y2, calculating a first remainder $y1 \equiv r1+h(x, ID)b+ay2 \bmod q$, wherein a is a first secret key and b is a second secret key, thus to generate a digital signature (x, y1, y2) for the message m;

for a verifier, applying the first remainder x and the signer's identification ID to the hash function to generate h(x, ID); and

recovering the message m contained in the first remainder x by calculating a remainder $\equiv xg^{y1}v1^{y2}v2^{h(x, ID)} \bmod p$ wherein v1 is a first public key, $v1 \equiv g^{-a} \bmod p$, v2 is a second public key, $v2 \equiv g^{-b} \bmod p$, and verifying the validation of the digital signature (x, y1, y2) by confirming the contents of the recovered message.

3. A method for generating a digital signature with appendix and verifying the generated digital signature when system coefficients are g, q and p, wherein p and q are prime numbers different from each other, g is a natural number between 1 and p and a remainder obtained by dividing q^{th} power of g by p is 1, the method comprising the steps of:

for a signer, selecting a first random number r1, applying a message m and a signer's identification ID to a hash function to generate h(ID, m), by calculating a first remainder $x \equiv h(ID, m)g^{-r1} \bmod p$, and applying the first remainder x and the message m to the hash function to generate h(x, m);

selecting second and third random numbers r2 and r3, calculating a second remainder $r4 \equiv r1+ar2 \bmod q$, (wherein a is a first secret key, and calculating a third remainder $r5 \equiv ar3+b \bmod q$, wherein b is a second secret key;

calculating a fourth remainder $y1 \equiv r4+r5\ h(x, m) \bmod q$, and calculating a fifth remainder $y2 \equiv r2+r3\ h(x, m) \bmod q$, thus to generate a digital signature (x, y1, y2) for the message m;

for a verifier, applying the first remainder x and the message m to the hash function to generate h(x, m), and recovering h(ID, m) by calculating a sixth remainder $\equiv xg^{y1}v1^{y2}v2^{h(x, m)} \bmod p$, wherein v1 is a first public key, $v1 \equiv g^{-a} \bmod p$, v2 is a second public key and $v2 \equiv g^{-b} \bmod p$; and

verifying the validation of the digital signature (x, y1, y2) by confirming whether the recovered h(ID, m) is equal to h(x, ID) obtained by applying the signer's identification ID and the message m to the hash function.

4. A method for generating a digital signature with appendix and verifying the generated digital signature when system coefficients are g, q and p, wherein p and q are prime numbers different from each other, g is a natural number between 1 and p and a remainder obtained by dividing q^{th} power of g by p is 1, the method comprising the steps of:

for a signer, selecting a first random number r1, applying a message m and a signer's identification ID to a hash function to generate h(ID, m), calculating a first remainder $x \equiv h(ID, m)g^{-r1} \bmod p$, and applying the first remainder x and the message m to the hash function to generate h(x, m);

selecting a second random number r2 between 1 and q to be used as y2, calculating a second remainder $y1 \equiv r1+h(x,m)b+ay2 \bmod q$, wherein a is a first secret key and b is a second secret key, thus to generate a digital signature (x, y1, y2) for the message m;

for a verifier, applying the first remainder x and the message m to the hash function to generate h(x, m), and recovering h(ID, m) by calculating a sixth remainder $\equiv xg^{y1}v1^{y2}v2^{h(x, m)} \bmod p$, wherein v1 is a first public key, $v1\ g^{-a} \bmod p$, v2 is a second public key and $v2 \equiv g^{-b} \bmod p$ and

verifying the validation of the digital signature (x, y1, y2) by confirming whether the recovered h(ID, m) is equal to h(ID, m) obtained by applying the signer's identification ID and the message m to the hash function.

5. A method for authenticating user's identity when system coefficients are g, q and p, wherein p and q are prime numbers different from each other, g is a natural number between 1 and p and a remainder obtained by dividing qth power of g by p is 1, the method comprising the steps of:

for a prover, selecting a first random number r1, making out authentication information I including a prover's identification and a current time, transmitting a first remainder $x \equiv Ig^{-r1} \bmod p$, to a verifier, and for the verifier, transmitting a second random number e to the prover;

for the prover, applying the first remainder x and the second random number e to the hash function to yield h(x, e), selecting second and third random numbers r2 and r3, calculating a second remainder $r4 \equiv r1+ar2 \bmod$

q wherein a is a first secret key, and calculating a third remainder $r5 \equiv ar3+b \bmod q$, wherein b is a second secret key;

calculating a fourth remainder $y1 \equiv r4+r5\ h(x, e) \bmod q$, and calculating a fifth remainder $y2 \equiv r2+r3\ h(x, e) \bmod q$, thus to generate a digital signature (x, y1, y2) for the message m;

for a verifier, recovering the authentication information I contained in the first remainder x by calculating a remainder $\equiv xg^{y1}v1^{y2}v2^{h(x,\ ID)} \bmod p$, wherein v1 is a first public key $v1 \equiv g^{-a} \bmod p$, v2 is a second public key and $v2 \equiv g^{-b} \bmod p$, and authenticating prover's identity by confirming the contents of the recovered authentication information.

6. A method for authenticating user's identity as claimed in claim **5**, wherein said authentication information I is 1.

7. A method for authenticating user's identity when system coefficients are g, q and p, wherein p and q are prime numbers different from each other, g is a natural number between 1 and p and a remainder obtained by dividing q^{th} power of g by p is 1 the method comprising the steps of:

for a prover, selecting a first random number −r1, making out authentication information I including a prover's identification and a current time, transmitting a first remainder $x \equiv Ig^{r1} \bmod p$ to a verifier, and for the verifier, transmitting a second random number e to the prover;

for the prover, applying the first remainder x and the second random number e to the hash function to generate h(x, e), selecting second and third random numbers r2 and r3, calculating a second remainder $r4 \equiv -r1+ar2 \bmod q$, wherein a is a first secret key, and calculating a third remainder $r5 \equiv ar3+b \bmod q$, wherein b is a second secret key;

calculating a fourth remainder $y1 \equiv r4+r5\ h(x, e) \bmod q$, and calculating a fifth remainder $y2 \equiv r2+r3\ h(x, e) \bmod q$, thus to generate a digital signature (x, y1, y2) for the message m;

for a verifier, recovering the authentication information I contained in the first remainder x by calculating a remainder $\equiv xg^{y1}v1^{y2}v2^{h(x,\ e)} \bmod p$, wherein v1 is a first public key, $v1 \equiv g^{-a} \bmod p$, v2 is a second public and $v2 \equiv g^{-b} \bmod p$, and authenticating prover's identity by confirming the contents of the recovered authentication information.

8. A method for authenticating user's identity as claimed in claim **7**, wherein said authentication information I is 1.

9. A method for authenticating user's identity when system coefficients are g, q and p, wherein p and q are prime numbers different from each other, g is a natural number between 1 and p and a remainder obtained by dividing q^{th} power of g by p is 1, the method comprising the steps of:

for a prover, selecting a first random number r1, making out authentication information I including a prover's identification and a current time, transmitting a first remainder $x \equiv Ig^{-r1} \bmod p$, to a verifier, and for the verifier, transmitting a second random number e to the prover;

for the prover, applying the first remainder x and the second random number e to the hash function to generate h(x, e), selecting a random number r2 between 1 and q to be used as y2, calculating a first remainder $y1 \equiv r1+h(x, e)b+ay2 \bmod q$ wherein a is a first secret key and b is a second secret key, thus to generate a digital signature (x, y1, y2) for the message m;

for a verifer, recovering the authentication information I contained in the first remainder x by calculating a remainder $\equiv xg^{y1}v1^{y2}v2^{h(x,\ e)} \bmod p$, and authenticating prover's identity by confirming the contents of the recovered authentication information.

10. A method for authenticating user's identity as claimed in claim **9**, wherein said authentication information I is 1.

11. A method for authenticating user's identity when system coefficients are g, q and p, wherein p and q are prime numbers different from each other, g is a natural number between 1 and p and a remainder obtained by dividing q^{th} power of g by p is 1, the method comprising the steps of:

for a prover, selecting a first random number −r1, making out authentication information I including a prover's identification and a current time, transmitting a first remainder $x \equiv Ig^{r1} \bmod p$ to a verifier, and for the verifier, transmitting a second random number e to the prover;

for the prover, applying the first remainder x and the second random number e to the hash function to generate h(x, e), selecting a random number r2 between 1 and q as y2, calculating a first remainder $y1 \equiv -r1+h(x, e)b+ay2 \bmod q$, wherein a is a first secret key and b is a second secret key, thus to generate a digital signature (x, y1, y2) for the message m; and

for a verifier, recovering the authentication information I contained in the first remainder x by calculating a remainder $\equiv xg^{y1}v1^{y2}v2^{h(x,\ e)} \bmod p$, and authenticating prover's identity by confirming the contents of the recovered authentication information.

12. A method for authenticating user's identity as claimed in claim **11**, wherein said authentication information I is 1.

* * * * *

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 742 618**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **96 13973**

(51) Int Cl⁶ : H 04 L 12/22, H 04 L 9/32

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 15.11.96.

(30) **Priorité** : 17.05.95 KR 9512289.

(43) **Date de la mise à disposition du public de la demande :** 20.06.97 Bulletin 97/25.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés :** Division demand©e le 15/11/96 b©n©ficiant de la date de d©pét du 17/05/96 de la demande initiale nÊ 96 06154

(71) **Demandeur(s) :** *KOREA TELECOM* — KR.

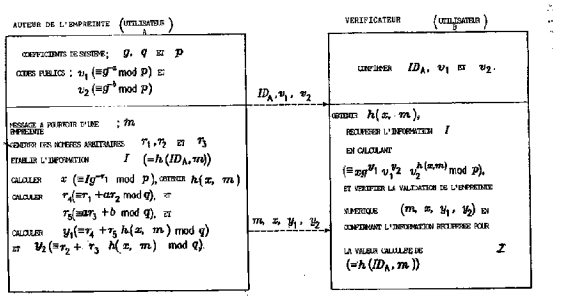
(72) **Inventeur(s) :** AHN KEUM HYUG, LEE YUN HO, PARK ILL HWAN et JANG CHUNG RYONG.

(73) **Titulaire(s) :**

(74) **Mandataire :** CABINET MALEMONT.

(54) SYSTEME D'EMPREINTE NUMERIQUE AVEC APPENDICE.

(57) La présente invention concerne un procédé pour générer une empreinte numérique avec appendice et pour vérifier l'empreinte numérique générée, pour authentifier chaque information de traitement d'identité, protéger l'intégrité de l'information transférée et empêcher le traitement d'informations frauduleuses.



FR 2 742 618 - A1

Système d'empreinte numérique avec appendice

La présente invention concerne un système d'empreinte numérique permettant une récupération de message, et un système d'empreinte numérique avec appendice pour authentifier chaque information de traitement d'identité, protéger l'intégrité de l'information transférée et empêcher le traitement d'informations frauduleuses.

Une empreinte numérique correspondant à une empreinte manuelle classique sert à confirmer un interlocuteur, à empêcher la modification non autorisée du contenu de la communication et à résoudre un litige concernant une attitude de communication. Un procédé destiné à générer l'empreinte numérique peut comprendre un système d'empreinte numérique avec appendice ou un système d'empreinte numérique permettant une récupération de message, suivant les formes et les fonctions de l'empreinte numérique générée.

Si on suppose que p désigne un nombre premier élevé, q un autre nombre premier destiné à diviser p−1, g un entier naturel ayant un reste 1 obtenu grâce à la division de sa puissance q par p, g se situant entre 1 et p, alors g, q et p sont des coefficients de système couramment utilisés par les utilisateurs. Si chaque utilisateur choisit au hasard comme code secret un entier naturel s situé entre 1 et q et utilise comme code public un reste v ($\equiv g^{-s} \bmod p$) obtenu en divisant la puissance −s de g par p, les coefficients publics utilisés par chaque utilisateur sont v, g, q et p.

Il est difficile de trouver le code secret s parmi ces coefficients publics, et un problème de logarithmes discrets est donc difficile à calculer. De nombreux systèmes d'identification de codes publics et de nombreux systèmes d'empreinte numérique sont basés sur le degré de sécurité, du fait que le problème des logarithmes discrets est difficile à calculer.

En 1989, Schnorr a divulgué le système d'identification et le système d'empreinte numérique basés sur la sécurité des logarithmes discrets. Le système d'empreinte numérique divulgué par Schnorr, qui est le système d'empreinte numérique avec appendice, apporte à celui qui avait été divulgué en

1985 par Elgamal une fonction de compression par hachage et simplifie la procédure destinée à générer et à vérifier l'empreinte numérique. De plus, l'empreinte numérique générée est de petite taille.

Le système d'identification proposé par Schnorr utilise la même structure de logarithme que le système d'empreinte numérique, et il authentifie la propre identité d'une personne face à un interlocuteur.

Le système d'identification proposé par Schnorr, selon lequel un fournisseur de preuve A authentifie son identité face à un vérificateur B, va maintenant être décrit.

Si les coefficients de système du fournisseur de preuve sont g, q et p, le code secret s ($1 < s < q$) et le code public v ($\equiv g^{-s} \bmod p$), le fournisseur de preuve A choisit un nombre arbitraire r situé entre 1 et q et transmet au vérificateur B un reste x ($\equiv g^r \bmod p$) obtenu en divisant la puissance r de g par p. Si x est reçu du fournisseur de preuve A, le vérificateur B choisit un nombre arbitraire e situé entre 1 et q et transmet le nombre e au fournisseur de preuve A. Le fournisseur de preuve multiplie le nombre arbitraire e reçu du vérificateur B par le code secret s et additionne le nombre arbitraire r afin d'obtenir r+se. Le fournisseur de preuve A transmet au vérificateur B un reste y ($\equiv r+se \bmod q$) obtenu en divisant r+se par q. Si y est reçu du fournisseur de preuve A, le vérificateur B calcule un reste x' ($\equiv g^y v^e \bmod p$) obtenu en divisant le produit de la puissance y de g et de la puissance e de v par p. Le vérificateur B authentifie la validation de l'identité du fournisseur de preuve en confirmant que x' et x sont égaux.

Dans le système d'empreinte numérique avec appendice proposé par Schnorr, si un message à pourvoir d'une empreinte est m, l'auteur de l'empreinte A choisit un nombre arbitraire r situé entre 1 et q et calcule un reste x ($\equiv g^r \bmod p$) obtenu en divisant la puissance r de g par p. Le message m et le reste x calculé sont soumis à la fonction de hachage afin d'obtenir e (= h(x, m)). L'auteur de l'empreinte A calcule un reste y ($\equiv r+se \bmod q$) obtenu en divisant r, additionné au produit de s et e, par q. (e, y) est alors l'empreinte numérique avec appendice pour le message m. La validation de l'empreinte numérique (e, y) avec

appendice pour le message m est facilement vérifiée puisqu'on connaît un code public.

Cela veut dire que si l'empreinte numérique avec appendice de l'auteur de l'empreinte A pour le message m est (e, y), le vérificateur B calcule un reste x' ($\equiv g^y v^e \bmod p$) obtenu en divisant le produit de la puissance y de g et de la puissance e de v par p. Le reste x' et le message m sont soumis à la fonction de hachage afin d'obtenir e' (= h(x', m). La validation de l'empreinte numérique (e, y) avec appendice de l'auteur de l'empreinte A est vérifiée grâce à une confirmation que e' et e sont égaux.

Depuis, Nyberg et Rueppel ont divulgué en 1993 le système d'empreinte numérique permettant une récupération de message et basé sur la sécurité des logarithmes discrets. Le système d'empreinte numérique permettant une récupération de message de N-R (Nyberg-Rueppel) va maintenant être décrit.

On suppose que les coefficients de système de l'auteur de l'empreinte sont g, q et p, que le code secret est s ($1 < s < q$), la clé publique v ($\equiv g^{-s} \bmod p$) et le message à pourvoir d'une empreinte m, m étant un entier naturel supérieur ou égal à 1 et inférieur ou égal au nombre premier p. L'auteur de l'empreinte choisit un nombre arbitraire r situé entre 1 et q et calcule un reste x ($\equiv mg^{-r} \bmod p$) obtenu en divisant le produit du message m et de la puissance -r de g par p. L'auteur de l'empreinte additionne r au code secret s multiplié par x afin d'obtenir r+sx, et calcule un reste y ($\equiv r+sx \bmod q$) obtenu en divisant r+sx par q. (x, y) est alors l'empreinte numérique permettant une récupération de message pour le message m.

Pour vérifier l'empreinte numérique (x, y), le vérificateur calcule un reste ($\equiv xg^y v^x \bmod p$) obtenu en divisant le produit de x, de la puissance y de g et de la puissance x de v par p afin de récupérer le message m. Le vérificateur vérifie la validation de l'empreinte numérique (x, y) en confirmant le contenu du message m récupéré.

Cependant, l'empreinte numérique avec appendice génère seulement l'empreinte numérique pour le message. Dans l'empreinte numérique permettant

une récupération de message, si le message à pourvoir d'une empreinte est supérieur en taille à p, le message doit être divisé en différents messages inférieurs à p. Etant donné que l'empreinte numérique est générée pour les messages divisés, cela augmente la taille de l'empreinte numérique générée.

La présente invention a donc pour but de proposer un système d'empreinte numérique avec appendice destiné à confirmer la modification non autorisée d'un message et à détecter le comportement de transmission.

Le but de l'invention est atteint par un procédé pour générer une empreinte numérique avec appendice et pour vérifier l'empreinte numérique générée, lorsque les coefficients de système sont g, q et p, caractérisé par les phases suivantes :

sélection (par l'auteur d'une empreinte) d'un premier nombre arbitraire r1, application d'une fonction de hachage pour un message m et une identification ID de l'auteur de l'empreinte afin d'obtenir h(ID, m), calcul d'un premier reste x ($\equiv h(ID, m)\ g^{-r1} \bmod p$) obtenu en divisant le produit de h(ID, m) et de la puissance –r1 de g par p, et application de la fonction de hachage pour le premier reste x et ledit message m afin d'obtenir h (x, m) ;

sélection d'un deuxième et d'un troisième nombre arbitraire r2 et r3, calcul d'un deuxième reste r4 ($\equiv r1 + ar2 \bmod q$) obtenu en divisant par q le premier nombre arbitraire r1 additionné au produit d'un premier code secret a et du deuxième nombre arbitraire r2, et calcul d'un troisième reste r5 ($\equiv ar3 + b \bmod q$) obtenu en divisant par q un second code secret b additionné au produit du premier code secret a et du troisième nombre arbitraire r3 ;

calcul d'un quatrième reste y1 ($\equiv r4 + r5\ h(x, m) \bmod q$) obtenu en divisant par q le deuxième reste r4 additionné au produit du troisième reste r5 et de h(x, m), et calcul d'un cinquième reste y2 ($\equiv r2 + r3\ h(x, m) \bmod q$) obtenu en divisant par q le deuxième nombre arbitraire r2 additionné au produit du troisième nombre arbitraire r3 et de h(x, m), pour générer ainsi une empreinte numérique (x, y1, y2) pour le message m ;

application (par un vérificateur) de la fonction de hachage pour le premier reste x et le message m afin d'obtenir h(x, m), et récupération de h(ID,

m) grâce au calcul d'un sixième reste ($\equiv xg^{y1}v1^{y2}v2^{h(x,m)} \bmod p$) obtenu en divisant par p le produit du premier reste x, de la puissance y1 de g, de la puissance y2 d'un premier code public v1 ($\equiv g^{-a} \bmod p$) et de la puissance {h(x, ID)} d'un second code public v2 ($\equiv g^{-b} \bmod p$) ; et

vérification de la validation de l'empreinte numérique (x, y1, y2) grâce à la confirmation que la valeur h(ID, m) récupérée est égale à la valeur h(x, ID) obtenue grâce à l'application de la fonction de hachage pour l'identification ID de l'auteur de l'empreinte et le message m.

La présente invention va être décrite plus en détail en référence aux dessins joints.

La figure 1 montre un traitement pour un système d'empreinte numérique permettant une récupération de message selon la présente invention,

la figure 2 montre un traitement pour un système d'empreinte numérique avec appendice selon la présente invention, et

la figure 3 montre un traitement pour un système d'identification selon la présente invention.

Selon la figure 1, chaque utilisateur a deux codes secrets et deux codes publics correspondant à ceux-ci, et peut générer une empreinte numérique pour un message à pourvoir d'une empreinte. Si le message à pourvoir d'une empreinte est m, les codes secrets de l'auteur de l'empreinte a et b et les codes publics v1 ($\equiv g^{-a} \bmod p$) et v2 ($\equiv g^{-b} \bmod p$), chaque utilisateur utilise couramment une fonction de hachage h et des coefficients de système g, q et p. Pendant l'utilisation d'un système d'empreinte numérique, une identification unique (ID) est attribuée à chaque utilisateur à partir d'un centre d'authentification de code.

Un auteur d'empreinte A choisit un nombre arbitraire r1 situé entre 1 et q et calcule un reste x ($\equiv mg^{-r1} \bmod p$) obtenu en divisant le produit du message m et de la puissance −r de g par p. Il soumet le reste x et son identification ID_A à la fonction de hachage afin d'obtenir $h(x, ID_A)$. Il choisit des nombres arbitraires r2 et r3 situés entre 1 et q et calcule r4 ($\equiv r1 + ar2 \bmod q$),

r5 ($\equiv$ ar3 + b mod q), y1 ($\equiv$ r4 + h(x, ID_A)r5 mod q), et y2 ($\equiv$ r2 + h(x, ID_A)r3 mod q).

Au lieu de calculer y1 et y2 en utilisant h(x, ID_A) après avoir choisi r2 et r3 et après avoir calculé r4 et r5 à l'aide des codes secrets a et b, on peut choisir comme valeur de y2 un nombre arbitraire r2 et calculer y1 en utilisant les codes secrets a et b et la valeur calculée pour h(x, ID_A). Cela veut dire que l'auteur de l'empreinte A choisit le nombre arbitraire r2 situé entre 1 et q comme valeur de y2. Puis y1 est calculé à l'aide de la formule y1 $\equiv$ r1 + h(x, ID_A)b + ay2 mod q. La valeur (x, y1, y2) obtenue est donc l'empreinte numérique permettant une récupération de message pour le message m.

Pour vérifier l'empreinte numérique (x, y1, y2), un vérificateur B soumet x et l'identification ID_A de l'auteur de l'empreinte à la fonction de hachage afin d'obtenir h(x, ID_A). On récupère le message m en calculant un reste ($\equiv xg^{y1}v1^{y2}v2^{h(x,IDA)}$ mod p) obtenu en divisant par p le produit de x, de la puissance y1 de g, de la puissance y2 du code public v1 et de la puissance {h(x, ID_A)} du code public v2. Le vérificateur B vérifie la validation de l'empreinte pour le message m en confirmant le contenu du message m récupéré.

Selon la figure 2, l'empreinte numérique générée est ajoutée à la fin d'un message pourvu d'une empreinte et est traitée par paire avec ce message.

L'auteur de l'empreinte A soumet son identification ID_A et le message m à la fonction de hachage afin d'obtenir I (= h(ID_A, m)). Il établit également I en annexant les données relatives à la sécurité, par exemple la description pour le message correspondant et l'heure à laquelle l'empreinte numérique est générée par un terminal d'ordinateur. Il choisit un nombre arbitraire r1 situé entre 1 et q et calcule un reste x ($\equiv Ig^{-r1}$ mod p) obtenu en divisant le produit de I et de la puissance −r1 de g par p. Il soumet x et le message m à la fonction de hachage afin d'obtenir h(x, m). Il choisit enfin des nombres arbitraires r2 et r3 situés entre 1 et q et calcule r4 ($\equiv$ r1 + ar2 mod q), r5 ($\equiv$ ar3 + b mod q), y1 ($\equiv$ r4 + h(x, m)r5 mod q) et y2 ($\equiv$ r2 + h(x, m)r3 mod q).

Au lieu de calculer y1 et y2 en utilisant h(x, m) après avoir choisi les nombres arbitraires r2 et r3 et après avoir calculé r4 et r5 à l'aide des codes

secrets a et b, on peut choisir comme valeur de y2 un nombre arbitraire r2 et calculer y1 en utilisant les codes secrets a et b et h(x, m) : l'auteur de l'empreinte A choisit comme valeur de y2 les nombres arbitraires r2 entre 1 et q. Le reste y1 est calculé à l'aide de la formule $y1 \equiv r1 + h(x, m)b + ay2 \bmod q$. (x, y1, y2) est ainsi l'empreinte numérique avec appendice pour le message m et est traitée avec celui-ci sous la forme (m, x, y1, y2).

Pour vérifier l'empreinte numérique (m, x, y1, y2) avec appendice, le vérificateur B calcule h(x, m) en soumettant x et le message m dans l'empreinte numérique (m, x, y1, y2) à la fonction de hachage. On récupère I en calculant un reste ($\equiv xg^{y1}v1^{y2}v2^{h(x,m)} \bmod p$) obtenu en divisant par p le produit de x, de la puissance y1 de g, de la puissance y2 de v1 et de la puissance (h(x,m)) de v2. Le vérificateur B soumet l'identification ID_A de l'auteur de l'empreinte et le message m à la fonction de hachage afin d'obtenir $h(ID_A, m)$. On vérifie la validation de l'empreinte numérique avec appendice pour le message m en confirmant que la valeur obtenue pour $h(ID_A, m)$ est égale à la valeur récupérée pour I.

En conséquence, l'empreinte numérique permettant une récupération de message et l'empreinte numérique avec appendice sont utilisées d'une manière appropriée en fonction de la longueur de la séquence binaire du message à pourvoir d'une empreinte. Si la taille du message est petite, l'auteur de l'empreinte utilise l'empreinte numérique permettant une récupération de message. Etant donné que le vérificateur peut récupérer le message pourvu d'une empreinte à partir du résultat de la vérification de la validation de l'empreinte numérique, l'importance de la communication entre l'auteur de l'empreinte et le vérificateur peut être réduite. Si la taille du message est grande, l'empreinte numérique avec appendice est utilisée pour générer l'empreinte numérique comprenant des informations comme une phrase de description de l'auteur de l'empreinte, une heure d'empreinte, etc.

Cela veut dire que l'auteur de l'empreinte soumet son identification ID et le message m à la fonction de hachage afin d'obtenir h(ID, m). Il annexe à h(ID, m) la phrase de description pour le message m. Il établit I (= $h(ID_A, m)$, une

phrase de description et une heure d'empreinte) en annexant la description pour le message correspondant et l'heure à laquelle l'empreinte numérique est générée par un terminal d'ordinateur, et génère l'empreinte numérique avec appendice.

Selon la figure 3, pour améliorer la sécurité, chaque utilisateur peut utiliser deux codes secrets et deux codes publics correspondant à ceux-ci. Des nombres arbitraires a et b sont choisis entre 1 et q comme codes secrets. Les codes publics sont v1 ($\equiv g^{-a} \bmod p$) et v2 ($\equiv g^{-b} \bmod p$). Pour prouver sa propre identité à un vérificateur B, le fournisseur de preuve A choisit un nombre arbitraire r1 situé entre 1 et q et calcule la puissance -r1 de g. Le fournisseur de preuve A établit l'information I (= ID_A, date et heure d'empreinte, adresse du terminal utilisé, etc.) contenant son identification ID_A, la date et l'heure d'empreinte, une adresse d'ordinateur central ou une adresse de noeud indiquant une position d'un terminal utilisé, etc., et transmet x ($\equiv Ig^{-r1} \bmod p$) au vérificateur B. L'information d'authentification I peut être 1.

Si x est reçu du fournisseur de preuve A, le vérificateur B choisit un nombre arbitraire e situé entre 1 et q et transmet le nombre arbitraire e au fournisseur de preuve A. Celui-ci soumet e et x à la fonction de hachage afin d'obtenir h(x, e). Les nombres r2 et r3 situés entre 1 et q sont choisis au hasard par le fournisseur de preuve A tandis que r4 ($\equiv$ r1 + ar2 mod q) et r5 ($\equiv$ ar3 + b mod q) sont calculés. Le fournisseur de preuve A transmet y1 ($\equiv$ r4 + h(x, e)r5 mod q) et y2 ($\equiv$ r2 + h(x, e)r3 mod q) au vérificateur B.

Dans la description précédente, on calcule y1 et y2 en utilisant h(x, e) après avoir choisi les nombres arbitraires r2 et r3 et après avoir calculé r4 et r5 en utilisant les codes secrets a et b. Cependant, on peut choisir comme valeur de y2 un nombre arbitraire r2 et calculer y1 en utilisant a et b et h(x, e) : le fournisseur de preuve A choisit comme valeur de y2 le nombre arbitraire r2 entre 1 et q, et le reste y1 est obtenu grâce à la formule y1 $\equiv$ r1 + h(x, e)b + ay2 mod q). Le fournisseur de preuve A transmet y1 et y2 au vérificateur B.

Si y1 et y2 sont reçus du fournisseur de preuve A, le vérificateur B récupère l'information d'authentification I en calculant $xg^{y1}v1^{y2}v2^{h(x,e)} \bmod p$. Le

vérificateur B authentifie l'identité du fournisseur de preuve en confirmant le contenu de l'information d'authentification I récupérée.

D'autre part, le nombre arbitraire –r1 peut être utilisé à la place du nombre arbitraire r1.

Comme on l'a décrit plus haut, le service d'information fiable est possible et un interlocuteur peut être efficacement authentifié.

REVENDICATIONS

1. Procédé pour générer une empreinte numérique avec appendice et pour vérifier l'empreinte numérique générée, lorsque les coefficients de système sont g, q et p, caractérisé par les phases suivantes :

sélection (par l'auteur d'une empreinte) d'un premier nombre arbitraire r1, application d'une fonction de hachage pour un message m et une identification ID de l'auteur de l'empreinte afin d'obtenir h(ID, m), calcul d'un premier reste x ($\equiv h(ID, m)\, g^{-r1} \bmod p$) obtenu en divisant le produit de h(ID, m) et de la puissance −r1 de g par p, et application de la fonction de hachage pour le premier reste x et ledit message m afin d'obtenir h (x, m) ;

sélection d'un deuxième et d'un troisième nombre arbitraire r2 et r3, calcul d'un deuxième reste r4 ($\equiv r1 + ar2 \bmod q$) obtenu en divisant par q le premier nombre arbitraire r1 additionné au produit d'un premier code secret a et du deuxième nombre arbitraire r2, et calcul d'un troisième reste r5 ($\equiv ar3 + b \bmod q$) obtenu en divisant par q un second code secret b additionné au produit du premier code secret a et du troisième nombre arbitraire r3 ;

calcul d'un quatrième reste y1 ($\equiv r4 + r5\, h(x, m) \bmod q$) obtenu en divisant par q le deuxième reste r4 additionné au produit du troisième reste r5 et de h(x, m), et calcul d'un cinquième reste y2 ($\equiv r2 + r3\, h(x, m) \bmod q$) obtenu en divisant par q le deuxième nombre arbitraire r2 additionné au produit du troisième nombre arbitraire r3 et de h(x, m), pour générer ainsi une empreinte numérique (x, y1, y2) pour le message m ;

application (par un vérificateur) de la fonction de hachage pour le premier reste x et le message m afin d'obtenir h(x, m), et récupération de h(ID, m) grâce au calcul d'un sixième reste ($\equiv x g^{y1} v1^{y2} v2^{h(x,m)} \bmod p$) obtenu en divisant par p le produit du premier reste x, de la puissance y1 de g, de la puissance y2 d'un premier code public v1 ($\equiv g^{-a} \bmod p$) et de la puissance {h(x, m)} d'un second code public v2 ($\equiv g^{-b} \bmod p$) ; et

vérification de la validation de l'empreinte numérique (x, y1, y2) grâce à la confirmation que la valeur h(ID, m) récupérée est égale à la valeur h(x, ID)

obtenue grâce à l'application de la fonction de hachage pour l'identification ID de l'auteur de l'empreinte et le message m.

2. Procédé pour générer une empreinte numérique avec appendice et pour vérifier l'empreinte numérique générée, lorsque les coefficients de système sont g, q et p, caractérisé par les phases suivantes :

sélection (par l'auteur d'une empreinte) d'un premier nombre arbitraire r1, application d'une fonction de compression par hachage pour un message m et une identification ID de l'auteur de l'empreinte afin d'obtenir h(ID, m), calcul d'un premier reste x ($\equiv h(ID, m)\ g^{-r1} \bmod p$) obtenu en divisant le produit de h(x, m) et de la puissance −r1 de g par p, et application de la fonction de hachage pour le premier reste x et ledit message m afin d'obtenir h (x, m) ;

sélection du deuxième nombre arbitraire r2 entre 1 et q comme valeur de y2, calcul d'un premier reste y1 ($\equiv r1 + h(x, m)b + ay2 \bmod q$) obtenu en divisant par q le premier nombre arbitraire r1 additionné au produit d'un premier code secret a et de y2 et au produit d'un second code secret b et de h(x, m), pour générer ainsi une empreinte numérique (x, y1, y2) pour le message m ;

application (par un vérificateur) de la fonction de hachage pour le premier reste x et le message m afin d'obtenir h(x, m), et récupération de h(ID, m) grâce au calcul d'un sixième reste ($\equiv xg^{y1}v1^{y2}v2^{h(x,m)} \bmod p$) obtenu en divisant par p le produit du premier reste x, de la puissance y1 de g, de la puissance y2 d'un premier code public v1 ($\equiv g^{-a} \bmod p$) et de la puissance {h(x, m)} d'un second code public v2 ($\equiv g^{-b} \bmod p$) ; et

vérification de la validation de l'empreinte numérique (x, y1, y2) grâce à la confirmation que la valeur h(ID, m) récupérée est égale à la valeur h(ID, m) obtenue grâce à l'application de la fonction de hachage pour l'identification ID de l'auteur de l'empreinte et le message m.

FIG. 1

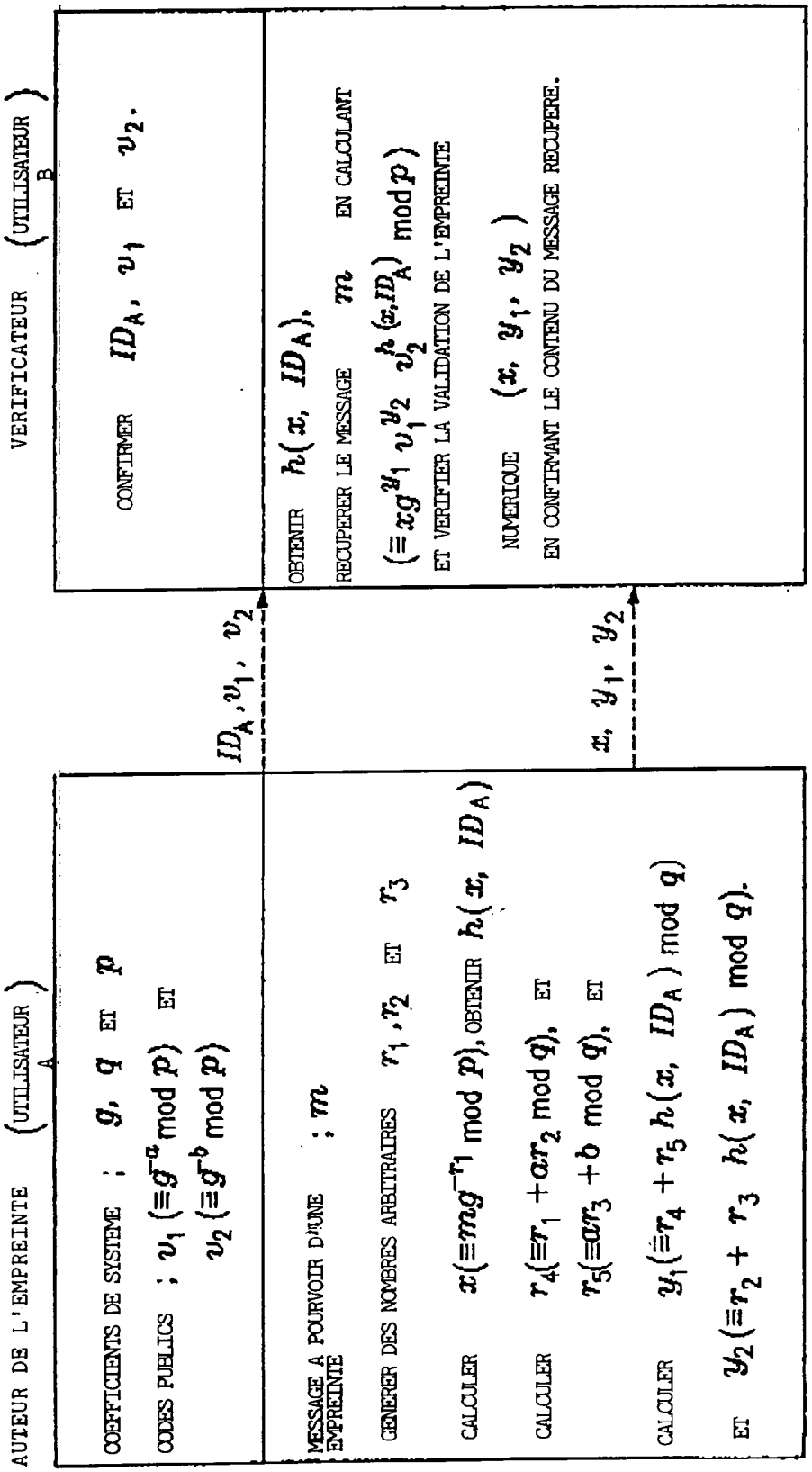

AUTEUR DE L'EMPREINTE (UTILISATEUR A)
VERIFICATEUR (UTILISATEUR B)
COEFFICIENTS DE SYSTEME : g, q ET p
CODES PUBLICS : v1 (≡g^a mod p) ET
v2 (≡g^b mod p)
CONFIRMER ID_A, v1 ET v2.
ID_A, v1, v2
MESSAGE A POURVOIR D'UNE EMPREINTE : m
GENERER DES NOMBRES ARBITRAIRES r1, r2 ET r3
CALCULER x(≡mg^-r1 mod p), OBTENIR h(x, ID_A)
CALCULER r4(≡r1 + ar2 mod q), ET
r5(≡ar3 + b mod q), ET
CALCULER y1(≡r4 + r5 h(x, ID_A) mod q)
ET y2(≡r2 + r3 h(x, ID_A) mod q).
x, y1, y2
OBTENIR h(x, ID_A),
RECUPERER LE MESSAGE m EN CALCULANT
(≡xg^y1 v1^y2 v2^h(x,ID_A) mod p)
ET VERIFIER LA VALIDATION DE L'EMPREINTE
NUMERIQUE (x, y1, y2)
EN CONFIRMANT LE CONTENU DU MESSAGE RECUPERE.

FIG. 2

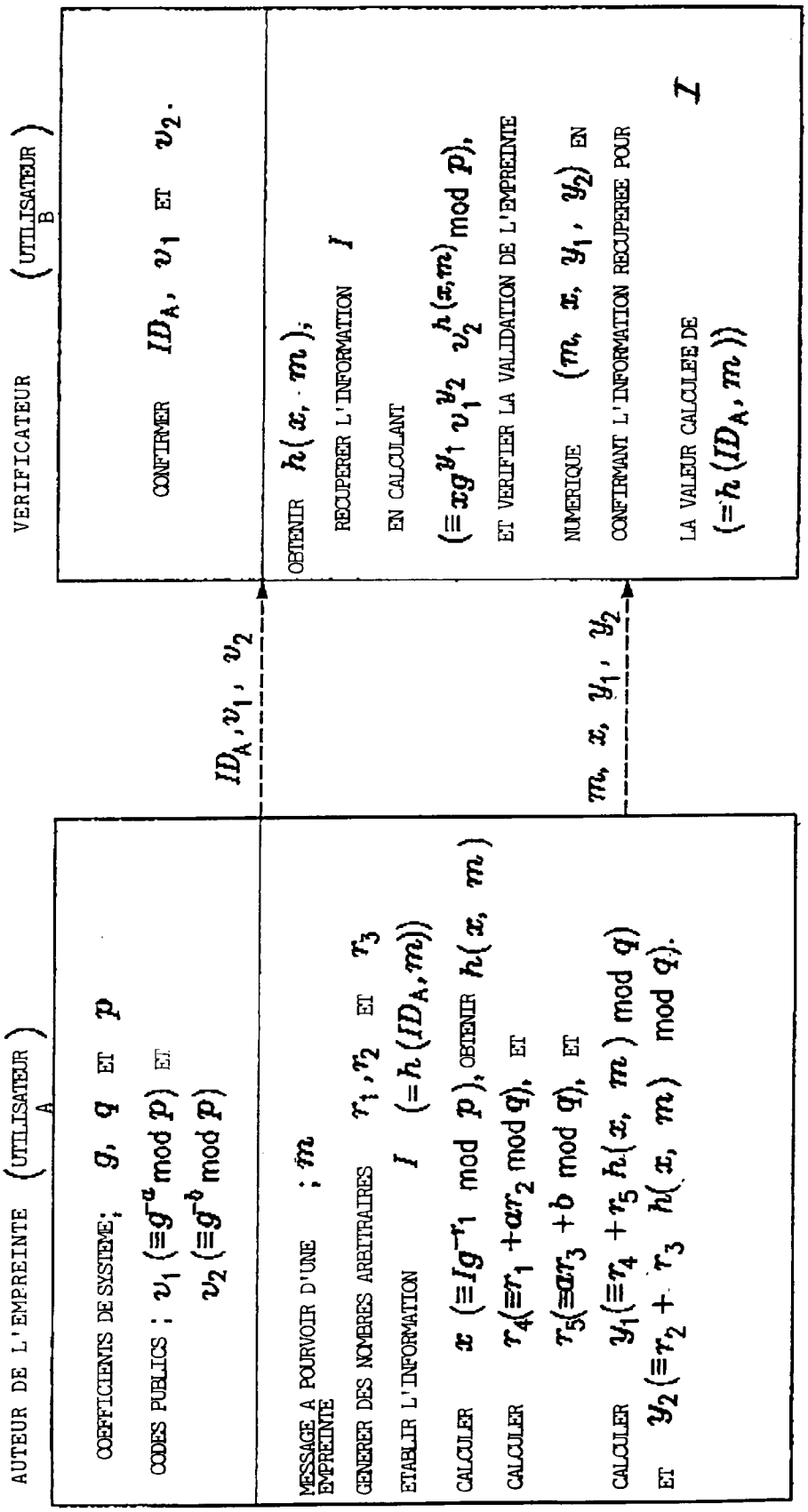
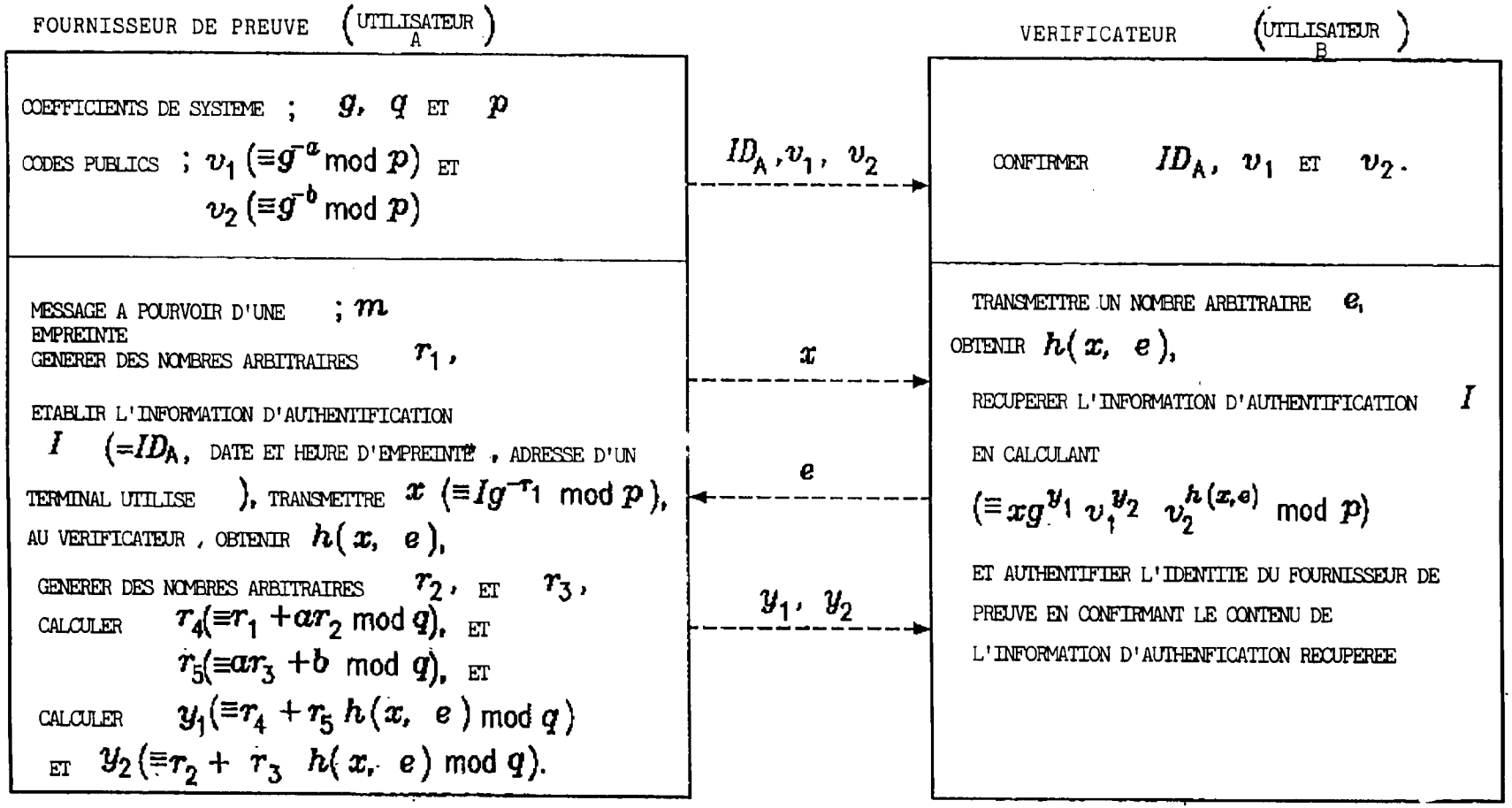

AUTEUR DE L'EMPREINTE (UTILISATEUR A)
COEFFICIENTS DE SYSTEME; g, q ET p
CODES PUBLICS ; v1 (≡g^-a mod p) ET
v2 (≡g^-b mod p)
MESSAGE A POUVOIR D'UNE EMPREINTE ; m
GENERER DES NOMBRES ARBITRAIRES r1, r2 ET r3
ETABLIR L'INFORMATION I (=h(IDA, m))
CALCULER x (≡Ig^-r1 mod p), OBTENIR h(x, m)
CALCULER r4(≡r1 +ar2 mod q), ET
r5(≡ar3 +b mod q), ET
CALCULER y1(≡r4 +r5 h(x, m) mod q)
ET y2 (≡r2 + r3 h(x, m) mod q).
IDA, v1, v2
m, x, y1, y2
VERIFICATEUR (UTILISATEUR B)
CONFIRMER IDA, v1 ET v2.
OBTENIR h(x, m);
RECUPERER L'INFORMATION I
EN CALCULANT
(≡xg^y1 v1^y2 v2^h(x,m) mod p),
ET VERIFIER LA VALIDATION DE L'EMPREINTE
NUMERIQUE (m, x, y1, y2) EN
CONFIRMANT L'INFORMATION RECUPEREE POUR
I
LA VALEUR CALCULEE DE
(=h(IDA, m))

FIG. 3



2742618